UNITED STATES DISTRICT COURT
DISTRICT OF MINNESOTA

UNITED STATES OF AMERICA,

Plaintiff,

v.

SHODIYA BABATUNDE and
JAMIU YINKA AHMED,

Defendants.

24CR256 DWF/TNL

**INDICTMENT**

18 U.S.C. § 1349
18 U.S.C. § 1343
18 U.S.C. § 1028A
18 U.S.C. § 1030(a)

THE GRAND JURY CHARGES THAT:

**Introduction**

1. At times relevant to the Indictment:

a. Defendants SHODIYA BABATUNDE and JAMIU YINKA AHMED were residents and citizens of Nigeria.

b. Fairview Health Services was a nonprofit health care company based in Minneapolis, Minnesota.

c. Optum Pay was an online health care payment system used by Fairview Health and other health care providers to receive payments and claims electronically. Optum Pay's servers were located in Minnesota.

d. Blue Cross & Blue Shield of Minnesota was a nonprofit health plan company based in Eagan, Minnesota.

e. Company A was a nonprofit health plan company based in Minneapolis, Minnesota.

f. Company B was a nonprofit health care provider and health insurance company based in Bloomington, Minnesota.

**Count One**
(Conspiracy to Commit Wire Fraud)

2. Paragraph 1 is re-alleged as if set forth herein.

3. Beginning in or about October 2020 and continuing through in or about 2024, in the State and District of Minnesota, and elsewhere,

SHODIYA BABATUNDE and
JAMIU YINKA AHMED,

did knowingly conspire with each other, and others known and unknown to the grand jury, to devise a scheme and artifice to defraud and to obtain money by materially false and fraudulent pretenses, representations, and promises, and for the purpose of executing such scheme and artifice, caused to be transmitted by means of a wire communication in interstate commerce, certain writings, signs, signals, and sounds, in violation of Title 18, United States Code, Sections 1343 and 1349.

4. Defendants BABATUNDE and AHMED carried out a fraudulent business email compromise scheme that targeted and deceived employees of several Minnesota-based health care companies, including Fairview Health, BlueCross BlueShield of Minnesota, Company A, and Company B, into making payments to bank accounts controlled by the defendants and their co-conspirators, rather than to the intended beneficiaries of the payments.

5. In furtherance of their fraudulent scheme, defendants BABATUNDE and AHMED created a fake "spoofed" internet domain called "fairviewhospitals.org"

and designed to appear as though it was controlled by Fairview Health. Defendants BABATUNDE and AHMED created this spoofed domain in order to fool Fairview Health employees into believing they were affiliated with Fairview Health.

6. Defendants BABATUNDE and AHMED used their spoofed domain to create email accounts designed to look as though they belonged to Fairview Health executives, including email accounts in the names of: (a) the CEO of Fairview Health; (b) the Executive Vice President and General Counsel of Fairview Health; and (c) a business analyst at Fairview Health.

7. Defendants BABATUNDE and AHMED used these spoofed email accounts to carry out a "phishing" scheme in which they sent emails purporting to be from Fairview Health executives to Fairview Health employees. The emails asked the Fairview Health employees to access an internet link and provide information such as names and passwords.

8. Defendants BABATUNDE and AHMED used the information they fraudulently obtained from Fairview Health employees to unlawfully obtain access to Fairview Health's Optum Pay account. Defendants BABATUNDE and AHMED then changed the banking information on vendor accounts in order to direct third-party vendors to transfer funds intended for Fairview Health into unauthorized bank accounts controlled by the defendants and their co-conspirators.

9. Defendants BABATUNDE and AHMED also used their spoofed Fairview Health email accounts to send emails purporting to be from Fairview Health executives to Fairview Health vendors, including BlueCross BlueShield of Minnesota,

Company A, and Company B. The emails requested that the vendors update the bank account information for payments to Fairview Health and provided new accounts into which such payments should be wired. Unbeknownst to the vendor companies, the new accounts were actually controlled by the defendants and their co-conspirators, not Fairview Health.

10. Defendants BABATUNDE and AHMED, and their co-conspirators, fraudulently induced Fairview Health vendors into making more than $13 million in payments to accounts controlled by defendants and their co-conspirators, including:

a. On or about July 29, 2020, BlueCross BlueShield of Minnesota made approximately 18 wire transfers totaling nearly $8 million to an account controlled by the defendants and their co-conspirators.

b. On or about November 19, 2020, Company B wired approximately $323,616 to an account controlled by the defendants and their co-conspirators.

c. On or about November 19, 2020, Company B wired approximately $743,494 to an account controlled by the defendants and their co-conspirators.

d. On or about November 25, 2020, Company A wired approximately $1,416,195 to an account controlled by the defendants and their co-conspirators.

e. On or about December 4, 2020, Company A wired approximately $1,412,045 to an account controlled by the defendants and their co-conspirators.

f. On or about December 24, 2020, Company B wired approximately $482,948 to an account controlled by the defendants and their co-conspirators.

11. In all, defendants BABATUNDE and AHMED, and their co-conspirators, fraudulently obtained more than $13 million from Minnesota-based health care companies through their scheme.

All in violation of Title 18, United States Code, Section 1349.

**Counts 2-7**
(Wire Fraud)

12. Paragraphs 1-11 are realleged and incorporated herein.

13. From at least in or about 2020 through in or about 2024, in the State and District of Minnesota, and elsewhere, the defendants,

SHODIYA BABATUNDE and
JAMUI YINKA AHMED,

and others known and unknown to the grand jury did knowingly devise and participate in a scheme and artifice to defraud and to obtain money by means of materially false and fraudulent pretenses, representations, and promises, and by concealment of material facts.

14. On or about the dates listed below, in the State and District of Minnesota and elsewhere, the defendants, as set forth below, for the purpose of executing the scheme described above, knowingly caused to be transmitted by means of a wire communication in interstate commerce, certain writings, signs, signals, and sounds, including the following:

| Count | Date (on or about) | Wire Details |
|---|---|---|
| 2 | July 29, 2020 | A $375,442 wire transfer from BlueCross BlueShield of Minnesota in Minnesota to an account controlled by defendants BABATUNDE and |

| | | |
|---|---|---|
| | | AHMED that passed through servers located outside the state of Minnesota |
| 3 | November 19, 2020 | A $323,616 wire transfer from Company B in Minnesota to an account controlled by defendants BABATUNDE and AHMED that passed through servers located outside the state of Minnesota |
| 4 | November 19, 2020 | A $743,494 wire transfer from Company B in Minnesota to an account controlled by defendants BABATUNDE and AHMED that passed through servers located outside the state of Minnesota |
| 5 | November 25, 2020 | A $1,416,195 wire transfer from Company A in Minnesota to an account controlled by defendants BABATUNDE and AHMED that passed through servers located outside the state of Minnesota |
| 6 | December 4, 2020 | A $1,412,045 wire transfer from Company A in Minnesota to an account controlled by defendants BABATUNDE and AHMED that passed through servers located outside the state of Minnesota |
| 7 | December 24, 2020 | A $482,948 wire transfer from Company B in Minnesota to an account controlled by defendants BABATUNDE and AHMED that passed through servers located outside the state of Minnesota |

All in violation of Title 18, United States Code, Sections 1343.

**Counts 8-10**
(Aggravated Identity Theft)

15. On or about the dates set forth below, in the state and District of Minnesota, and elsewhere, the defendant

SHODIYA BABATUNDE,

did knowingly use, without lawful authority, a means of identification of another person during and in relation to a felony violation enumerated in 18 U.S.C. § 1028A(c), namely wire fraud in violation of 18 U.S.C. § 1343, knowing that the means of identification belonged to another actual person.

| Count | Date | Employee Name | Employee Title |
|---|---|---|---|
| 8 | June 22, 2020 | Individual J.H. | President and Chief Executive Officer of *Fairview Health* |
| 9 | June 22, 2020 | Individual T.T. | Executive Vice President, Chief Administrative Officer, and General Counsel of Fairview Health |
| 10 | June 22, 2020 | Individual J.L. | Business Analyst at Fairview Health |

All in violation of Title 18, United States Code, Section 1028A.

**Counts 11-12**
(Computer Fraud)

16. On or about the dates set forth below, in the State and District of Minnesota, the defendant,

JAMIU YINKA AHMED,

knowingly and with intent to defraud accessed a protected computer without authorization, or exceeded authorized access, and by means of such conduct furthered an intended fraud and obtained something of value, namely, accessing Fairview Health servers to conduct fraudulent transactions that were not authorized by the account holders, as described in further detail below:

| Count | Date | Unauthorized Access |
|---|---|---|
| 11 | November 4, 2020 | Logged into Individual JG's Optum Pay account without authorization |
| 12 | November 4, 2020 | Logged into Individual JG's Optum Pay account without authorization |

All in violation of Title 18, United States Code, Section 1030(a)(4).

**Forfeiture Allegations**

17. If convicted of any of Counts 1 through 7 of this Indictment, the defendants shall forfeit to the United States, pursuant to Title 18, United States Code, Section 981(a)(1)(C) and Title 28, United States Code, Section 2461(c), any property, real or personal, which constitutes or is derived from proceeds traceable to Counts 1 through 7 of the Indictment.

18. If convicted of any of Counts 11 through 12 of this Indictment, the defendants shall also forfeit to the United States, pursuant to Title 18, United States Code, Section 982(a)(2), any property constituting, or derived from, proceeds the person obtained directly or indirectly, as the result of the computer fraud alleged in Counts 11 through 12, and pursuant to Title 18, United States Code, Section 1030(i), any property, real or personal, constituting or derived from, any proceeds obtained, directly or indirectly, as a result of the violations and any personal property used or intended to be used to commit or facilitate the commission of these violations, , including any equipment, software, or other technology, used or intended to be used to commit, facilitate the commission of Counts 11 through 12 of the Indictment.

19. If any of the above-described property is unavailable for forfeiture, the United States intends to seek the forfeiture of substitute property as provided for in Title 21, United States Code, Section 853(p), as incorporated by Title 28, United States Code, Section 2461(c) and Title 18, United States Code, Sections 982(b) and 2328(b).

A TRUE BILL

_____ _____

UNITED STATES ATTORNEY FOREPERSON